ANALYTIX AUDIT

AUDIT REPORT

MAR 2023

Security Assessment

Pepa Inu Router

April 1, 2023

Audit Status: Pass

Audit Edition: Advance

Table of Contents

1 Assessment Summary

2 Technical Findings Summary

3 Project Overview

3.1 Main Contract Assessed

4 Smart Contract Risk Checks

5 Contract Ownership

7 KYC Check

8 Smart Contract Vulnerability Checks

8.1 Smart Contract Vulnerability Details

8.2 Smart Contract Inheritance Details

8.3 Smart Contract Privileged Functions

9 Assessment Results and Notes(Important)

10 Social Media Check(Informational)

11 Technical Findings Details

12 Disclaimer

Assessment Summary

This report has been prepared for Pepa Inu Router on the Binance Smart Chain network. Analytix Audit provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts.

ANALYTIX AUDIT

Project Overview

Token Summary

Parameter	Result
Address	0x926C018E6ce73A463BDA99aBfBa50a7ea9aDa833
Name	Pepa Inu
Token Tracker	Pepa Inu (PEPA)
Decimals	0
Supply	0
Platform	Binance Smart Chain
compiler	v0.8.18+commit.87f61d96
Contract Name	PepaRouter
Optimization	Yes with 2000 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/address/0x926C018E6ce73A463BDA99aBfBa50a7ea9aDa833#code
Payment Tx	Corporate Account

ANALYTIX AUDIT

Main Contract Assessed
Contract Name

Name	Contract	Live
Pepa Inu	0x926C018E6ce73A463BDA99aBfBa50a7ea9aDa833	Yes

TestNet Contract was Not Assessed

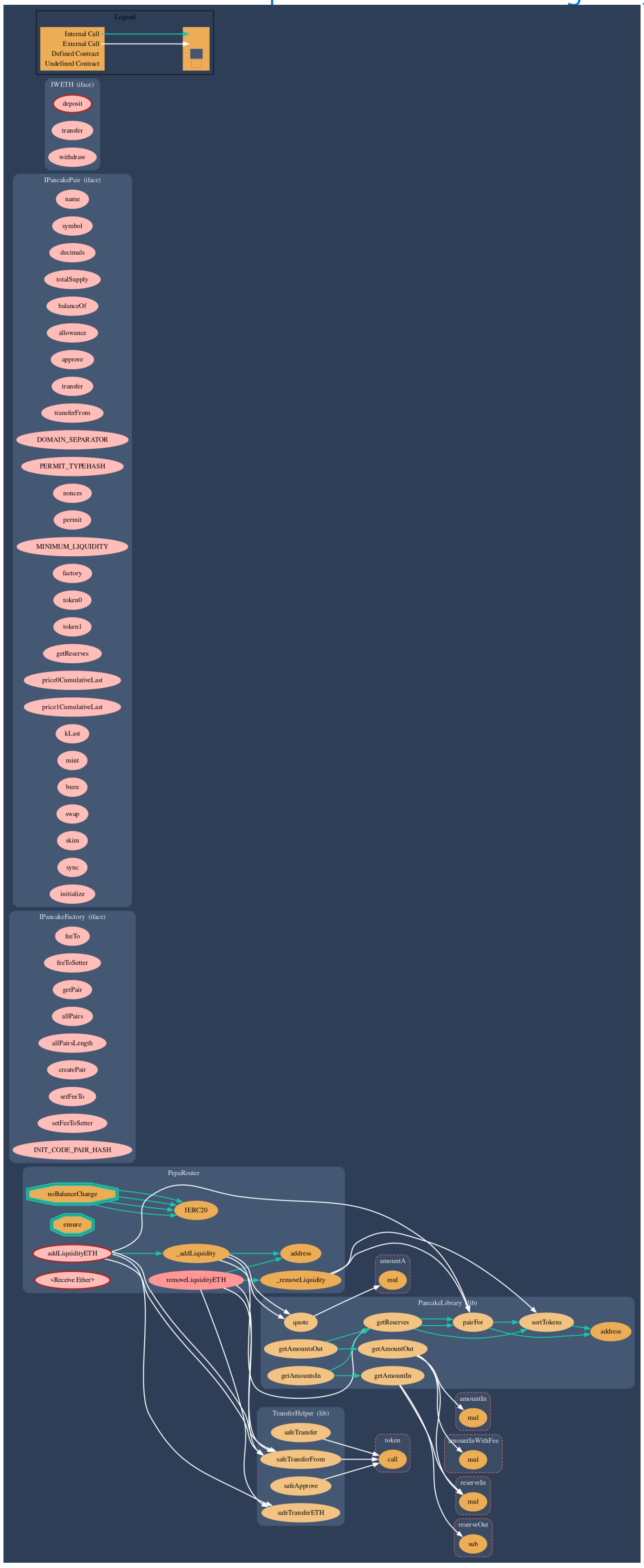
Solidity Code Provided

SolID	File Sha-1	FileName
PepaRouter	2a10a27f476b6a349e690c389a32386b3e1d8288	PepaRouter.sol
PepaRouter	0c3cb8c75c563d4040b6926ea189c43bcee80da05	IPancakeFactory.sol
PepaRouter	9d49ce9b084ce3db3eb079937293d4247ff97c57	IPancakePair.sol
PepaRouter	384ad507a226d1be559a878d8c7cda48cafa211f	IWETH.sol
PepaRouter	dd5c28f3df2600bb7c13eee468fe03f23543f0ac	PancakeLibrary.sol
PepaRouter	80bfc38afaba6fb5b17ce0b669d602ae694b238d	TransferHelper.sol

ANALYTIX
AUDIT

Call Graph

The contract for Pepa Inu has the following call graph structure.



KYC Information

The Project Owners of Pepa Inu is not KYC.

KYC Information Notes:

Auditor Notes:

Project Owner Notes:

Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	PepaRouter.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	PepaRouter.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	PepaRouter.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	PepaRouter.sol	L: 2 C: 0
SWC-104	Pass	Unchecked Call Return Value.	PepaRouter.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	PepaRouter.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	PepaRouter.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	PepaRouter.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	PepaRouter.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	PepaRouter.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	PepaRouter.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	PepaRouter.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	PepaRouter.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	PepaRouter.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	PepaRouter.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	PepaRouter.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	PepaRouter.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	PepaRouter.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	PepaRouter.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	PepaRouter.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	PepaRouter.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	PepaRouter.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	PepaRouter.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	PepaRouter.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	PepaRouter.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	PepaRouter.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	PepaRouter.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	PepaRouter.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	PepaRouter.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	PepaRouter.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	PepaRouter.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	PepaRouter.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	PepaRouter.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	PepaRouter.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	PepaRouter.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	PepaRouter.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	PepaRouter.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Smart Contract Vulnerability Details

SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

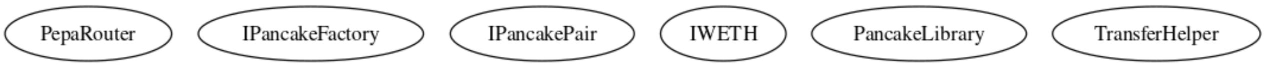
Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.

Inheritance

The contract for Pepa Inu has the following inheritance structure.



Smart Contract Advance Checks

ID	Severity	Name	Result	Status
PEPA-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
PEPA-02	Informational	Function Visibility Optimization	Fail	Pending
PEPA-03	Minor	Lack of Input Validation.	Pass	Pending
PEPA-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Found
PEPA-05	Major	Missing Event Emission.	Fail	Pending
PEPA-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Found
PEPA-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
PEPA-08	Major	Dead Code Elimination.	Pass	Not-Found
PEPA-09	Major	Third Party Dependencies.	Pass	Not Found
PEPA-10	Major	Initial Token Distribution.	Pass	Not-Found
PEPA-11	Minor	Missing Init_Hash for Pair Creation if needed.	Pass	Pending
PEPA-12	Major	Centralization Risks In The X Role	Pass	Not-Found
PEPA-13	Informational	Extra Gas Cost For User..	Pass	Not-Found
PEPA-14	Medium	Unnecessary Use Of SafeMath	Pass	Not-Found
PEPA-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found

ID	Severity	Name	Result	Status
PEPA-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found

PEPA-02 | Function Visibility Optimization.

Category	Severity	Location	Status
Gas Optimization	Informational	PepaRouter.sol: 66, 14	Pending

Description

The following functions are declared as public and are not invoked in any of the contracts contained within the projects scope:

Function Name	Parameters	Visibility
removeLiquidityETH		public

The functions that are never called internally within the contract should have external visibility

Remediation

We advise that the function's visibility specifiers are set to external, and the array-based arguments change their data location from memory to calldata, optimizing the gas cost of the function.

References:

external vs public best practices.

PEPA-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	🟠 Major	PepaRouter.sol: 38, 14	Pending

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.The linked code does not create an event for the transfer.

Remediation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Technical Findings Summary

Classification of Risk

Severity	Description
🔴 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
🟠 Major	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟡 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
🟢 Minor	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
ℹ️ Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
🔴 Critical	0	0	0
🟠 Major	1	1	0
🟡 Medium	0	0	0
🟢 Minor	1	1	1
ℹ️ Informational	1	1	0
Total	3	3	1

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/pepa_inu	Pass
Other	https://www.tiktok.com/@pepainu	Pass
Website	https://pepa-inu.com/	Pass
Telegram	https://t.me/pepa_inu	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Aduit Result

Final Audit Score

Review	Score
Security Score	87
Auditor Score	87

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Audit Passed

Current project reviewed successfully passed audit, meeting all requirements for approval per Analytix Audit guidelines.

@FreddyCryptos
Founder & CEO

Today's Date
Dubai - United Arab Emirates

Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- We review the current router and evaluated the current functions.
- customer adds liquidity and removes liquidity to PCS using Router.
- The router missing the init hash value that is standard on routers to create a pair, however, does not look like the customer will create the same.

Auditor Score =87
Audit Passed

Audit Passed

Current project reviewed successfully passed audit, meeting all requirements for approval per Analytix Audit guidelines.

@FreddyCryptos
Founder & CEO

Today's Date
Dubai - United Arab Emirates

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

Analytix Audit has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and Analytix Audit is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Analytix Audit or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Analytix Audit are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.